## 1. Volunerabilities

By definition Security vulnerabilities are defined as weaknesses in technology, software, or operational practices that can be exploited by threats, leading to potential risks such as unauthorized access or information leakage [1]. These vulnerabilities can tak on various forms and in this paper I will be focusing on open source tools designed for finding flaws in networks and web applications.

## 2. Classification

Classification of Common Vulnerabilities and Exposures(CVE) is provided by NVD which is using Common Weakness Enumeration(CWE) classification mechanism that differentiates CVEs by the type of vulnerability they represent. This classification distributes CVEs into a hierarchical structure CWE on higher level provide overview of volunerability type and can have many subtypes. CWE are classified based on their nature and effect. **https://nvd.nist.gov/vuln/categories**

## 3. Characteristics

**Cross-site request forgery**(csrf) is a volunerability that takes advantage of web application in which target is currently authenticated and by gaining the targets authentication token the attacker proceed to make actions as if they were the target. This attack can lead to anything from sending messages on victims behalf up to transfering money. In worst cases entire web applications can be compromised if user has high level of auhtorization.

## Bibliography

[1] "Security Vulnerability." [Online]. Available: **https://www.sciencedirect.com/topics/computer-science/security-vulnerability**

applications used Dirsearch,w3af,nikto,CloudSploit,Wapiti,Vega,Grabber w3af includes csrf testing